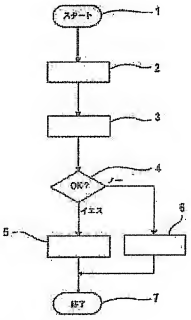
METHOD FOR ACTIVATING OR INACTIVATING AT LEAST A PART OF DATA STORED IN MEMORY DEVICE OF MICROCOMPUTER SYSTEM AND MICROCOMPUTER SYSTEM

Publication number: JP2003022218 (A)
Publication date: 2003-01-24
Inventor(s): SCHNEIDER KLAUS; ANGERBAUER RALF; HEINDL ALEXANDER +
Applicant(s): BOSCH GMBH ROBERT +
Classification:
- international: *G06F12/14; G06F21/00; G06F21/02; G06F21/24;* G06F12/14; G06F21/00; (IPC1-7): G06F12/14
- European: G06F21/00N1C; G06F21/00N1D1
Application number: JP20020155835 20020529
Priority number(s): DE20011026451 20010531

Also published as:
JP4344115 (B2)
DE10126451 (A1)
US2003018905 (A1)
US6948071 (B2)

Abstract of JP 2003022218 (A)

PROBLEM TO BE SOLVED: To surely and effectively prevent the use of data stored in a memory device which are illegally operated by a third unauthorized person. SOLUTION: This method comprises a step for encrypting the specific identifier of e microcomputer or for storing the signature of the specific identifier of the microcomputer in the preliminarily settable memory region of a memory device, a step for checking the signature of the identifier and/or for decoding the identifier at the time of starting the microcomputer system, and a step for activating or inactivating at least a part of the data depending on the checked result of the signature and/or the decoded identifier.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－22218
（P2003－22218Ａ）
(43)公開日　平成15年１月24日(2003.1.24)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３２０	Ｃ０６Ｆ　12/14	３２０Ｄ　５Ｂ０１７

審査請求　未請求　請求項の数15　ＯＬ　（全８頁）

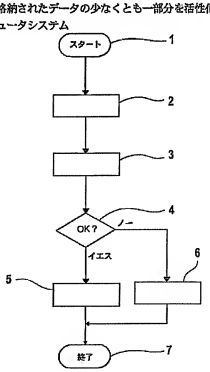
(21)出願番号　特願2002－155835(P2002－155835)
(22)出願日　平成14年５月29日(2002.5.29)
(31)優先権主張番号　１０１２６４５１．８
(32)優先日　平成13年５月31日(2001.5.31)
(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　390023711
ローベルト　ボッシュ　ゲゼルシャフト　ミット　ベシュレンクテル　ハフツング
ROBERT　BOSCH　GMBH
ドイツ連邦共和国　シュツットガルト　（番地なし）
(72)発明者　クラウス　シュナイダー
ドイツ連邦共和国　ルートヴィヒスブルク　ハンゼアテンシュトラーセ　22
(74)代理人　100061815
弁理士　矢野　敏雄　（外４名）

最終頁に続く

(54)【発明の名称】　マイクロコンピュータシステムのメモリ装置に格納されたデータの少なくとも一部分を活性化又は不活性化するための方法及びマイクロコンピュータシステム

(57)【要約】
【課題】　資格のない第三者によるメモリ装置に格納されたデータの不正操作の場合に、これらの不正操作されたデータの利用を確実にかつ効果的に阻止することである。
【解決手段】　上記課題は、マイクロコンピュータ固有の識別子は暗号化されるか又はマイクロコンピュータ固有の識別子の署名がメモリ装置の予め設定可能なメモリ領域に格納される方法ステップ、マイクロコンピュータシステムの起動の際に識別子の署名が検査され乃至は識別子が復号化される方法ステップ、署名の検査の結果に依存して乃至は復号化された識別子に依存してデータの少なくとも一部分が活性化又は不活性化される方法ステップによって解決される。



【特許請求の範囲】

【請求項１】　マイクロコンピュータシステム（３０）のメモリ装置（３２）に格納されたデータ（３３）の少なくとも一部分（３５、３６）を活性化又は不活性化するための方法において、

以下の方法ステップ、すなわちマイクロコンピュータ固有の識別子（１０）は暗号化されるか又は前記マイクロコンピュータ固有の識別子（１０）の署名（１５）が前記メモリ装置（３２）の予め設定可能なメモリ領域（３４）に格納される方法ステップ、

前記マイクロコンピュータシステム（３０）の起動の際に前記識別子（１０）の前記署名（１５）が検査され乃至は前記識別子（１０）が復号化される方法ステップ、

前記署名（１５）の検査の結果に依存して乃至は復号化された識別子（１０）に依存して前記データ（３３）の少なくとも一部分が活性化又は不活性化される方法ステップを特徴とする、マイクロコンピュータシステム（３０）のメモリ装置（３２）に格納されたデータ（３３）の少なくとも一部分（３５、３６）を活性化又は不活性化するための方法。

【請求項２】　データ（３３）の異なる部分（３５、３６）の活性化又は不活性化のために、様々な識別子がメモリ装置（３２）のメモリ領域（３４）に格納されることを特徴とする、請求項１記載の方法。

【請求項３】　データ（３３）の異なる部分（３５、３６）の活性化又は不活性化のために、識別子（１０）がメモリ装置（３２）の様々なメモリ領域（３４）に格納されることを特徴とする、請求項１又は２記載の方法。

【請求項４】　限定されたユーザグループだけがアクセスできるプライベート鍵（１４）に基づいてマイクロコンピュータ固有の識別子（１０、１５）が署名又は暗号化され、自由にアクセスできる公開鍵（１７）に基づいて前記識別子（１０）の署名（１５）が検査されるか乃至は前記識別子（１０）が復号化されることを特徴とする、請求項１～３のうちの１項記載の方法。

【請求項５】　識別子（１０、１５）はメモリ装置（３２）のメモリ領域（３４）に格納され、該メモリ領域（３４）はデータ（３３）の利用中には変更されないことを特徴とする、請求項１～４のうちの１項記載の方法。

【請求項６】　識別子（１０、１５）はメモリ領域（３４）に格納され、該メモリ領域（３４）はメモリ装置（３２）の再プログラミングの枠内でクリアされることを特徴とする、請求項１～５のうちの１項記載の方法。

【請求項７】　マイクロコンピュータシステム（３０）の起動毎に識別子（１０）の署名（１５）が検査されるか乃至は前記識別子（１０）が復号化されることを特徴とする、請求項１～６のうちの１項記載の方法。

【請求項８】　マイクロコンピュータシステム（３０）に割り当てられたシリアルナンバーはメモリ装置（３２）の予め設定可能なメモリ領域（３４）に署名されて又は暗号化されて格納されることを特徴とする、請求項１～７のうちの１項記載の方法。

【請求項９】　メモリ装置（３２）のメモリ領域（３４）に識別子（１０、１５）が格納されていない場合又はそこに格納された識別子（１０）の復号化がマイクロコンピュータシステム（３０）の起動時に失敗した場合、前記マイクロコンピュータシステム（３０）において前記メモリ装置（３２）に格納されたデータ（３３）の不正操作の検査のためのメカニズムが活性化されることを特徴とする、請求項１～８のうちの１項記載の方法。

【請求項１０】　メモリ装置（３２）のメモリ領域（３４）に格納された識別子（１０）の署名（１５）の検査又はそこに格納された識別子（１０）の復号化がマイクロコンピュータシステム（３０）の起動時に成功した場合、前記マイクロコンピュータシステム（３０）において前記メモリ装置（３２）に格納されたデータ（３３）の不正操作の検査のためのメカニズムが不活性化されることを特徴とする、請求項１～９のうちの１項記載の方法。

【請求項１１】　計算機器（３１）及びデータ（３３）が格納されているメモリ装置（３２）を有するマイクロコンピュータシステム（３０）において、

前記メモリ装置（３２）の予め設定可能なメモリ領域（３４）に署名されて又は暗号化されて格納されたマイクロコンピュータ固有の識別子（１０、１５）を有し、

前記マイクロコンピュータシステム（３０）の起動時に識別子（１０）の署名（１５）の検査のための乃至は前記識別子（１０）の復号化のための手段を有し、

前記マイクロコンピュータシステム（３０）の前記メモリ装置（３２）に格納された前記データ（３３）の少なくとも一部分（３５、３６）を、前記署名（１５）の検査の結果乃至は復号化された識別子（１０）に依存して活性化又は不活性化するための手段を有することを特徴とする、計算機器（３１）及びデータ（３３）が格納されているメモリ装置（３２）を有するマイクロコンピュータシステム（３０）。

【請求項１２】　マイクロコンピュータシステム（３０）は自動車機能の開ループ制御及び/又は閉ループ制御のための自動車のための制御機器として構成されていることを特徴とする、請求項１１記載のマイクロコンピュータシステム（３０）。

【請求項１３】　マイクロコンピュータシステム（３０）は請求項２～１０のうちの１項記載の方法を実施するための手段を有することを特徴とする、請求項１１又は１２記載のマイクロコンピュータシステム（３０）。

【請求項１４】　メモリ装置（３２）にはコンピュータプログラムが格納されており、該コンピュータプログラ

ムは計算機器（３１）において実行可能であり、請求項１～１０のうちの１項記載の方法の実施に適していることを特徴とする。請求項１１～１３のうちの１項記載のマイクロコンピュータシステム（３０）。

【請求項１５】　メモリ装置（３２）は計算機器（３１）と同一の半導体構成素子に形成されていることを特徴とする、請求項１１～１４のうちの１項記載のマイクロコンピュータシステム（３０）。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、マイクロコンピュータシステムのメモリ装置に格納されたデータの少なくとも一部分を活性化又は不活性化するための方法であって、とりわけそこに格納されたプログラムの一部分を活性化又は不活性化するための方法に関する。

【０００２】さらに本発明は、計算機器、とりわけマイクロプロセッサ及びデータ、とりわけプログラムが格納されているメモリ装置を有するマイクロコンピュータシステムに関する。

【０００３】

【従来の技術】従来技術からはマイクロコンピュータシステムのメモリ装置に格納されたデータ、とりわけそこに格納されたプログラムを不正操作から保護するための方法が公知である。このような方法は例えば自動車の制御機器に格納された制御プログラム又はそこに格納されたデータの資格のない不正操作を阻止するために使用される。制御プログラムは自動車における所定の機能、例えば内燃機関、走行ダイナミック制御、アンチロックシステム（ＡＢＳ）又は電子運転システム（ステア・バイ・ワイヤ（Steer-by-Wire））を開ループ制御又は閉ループ制御する。制御プログラムの不正操作のために、自動車の開ループ制御又は閉ループ制御されたユニットの故障が生じうる。それゆえ、制御プログラム又はデータの不正操作はできるだけ阻止されるべきであり、開ループ制御又は閉ループ制御されたユニットの故障の原因が検出されるか乃至は保証要求が正しく割り当てられるように、少なくとも不正操作が後から識別されるべきである。

【０００４】資格のない人物による制御プログラム又はデータの不正操作の危険にもかかわらず、制御機器のメモリ装置へのアクセスを完全に禁止することは有効ではない。例えば、制御機器の再プログラミングを行えるために、資格のあるユーザグループにはメモリ装置へアクセスすることが可能でなくてはならない。すなわち、例えばソフトウェアにおけるエラーを除去し又は新しい法的な基準値を顧慮するために、時々は制御プログラムの新しいバージョン又は新しいパラメータ又は限界値を制御機器に格納する必要がある。

【０００５】自動車制御機器ではスタンダード機器とアプリケーション機器との間で異なる。通常は制御機器はスタンダード機器として製造された後で市場に供給される。スタンダード機器の場合には、制御機器のメモリ装置に格納されたデータの不正操作の検査のためのメカニズムが活性化されている。不正操作されたデータはこれらのメカニズムによって通常識別され、これらのデータは阻止される。これらのメカニズムは全く異なるように構成することができる。従来技術からは様々な検査メカニズムが公知である。所定の状況、とりわけ制御機器の開発及びテストフェーズの間には、様々なデータが迅速かつ簡単にメモリ装置に格納されるように、検査メカニズムを不活性化する必要がある。不活性化された検査メカニズムを有する制御機器はアプリケーション機器と呼ばれる。

【０００６】メモリ装置に格納されたデータの完全なテストを保証するために、スタンダードの場合及びアプリケーションの場合に同一のデータ、とりわけ同一の制御プログラムが制御機器のメモリ装置に格納されていなければならない。それゆえ、他のデータをメモリ装置にロードする必要なしに、制御機器をスタンダードの場合からアプリケーションの場合に切り換えることができなくてはならない。制御機器の製造者によってテストされず認可されていない制御プログラムを持つ制御機器が市場に広まるのを阻止するために、アプリケーションの場合からスタンダードの場合へと戻る切り換えは望ましくなく、なるべくできないほうがよい。

【０００７】従来技術によれば、アプリケーション機器は制御機器のメモリ装置の秘密の不揮発性のメモリ領域におけるエントリによって特徴づけられる。この秘密のメモリ領域は制御機器の再プログラミングの枠内でプログラミングすべきメモリ装置のメモリ領域の外に存在する。スタンダード機器であるか又はアプリケーション機器であるかに応じて、秘密のメモリ領域はメモリ装置の最初のプログラミングに続いて乃至は相応の方法をきっかけにしてこの制御機器の起動の際に相応のエントリによってプログラミングされる。

【０００８】制御機器の次の起動の際には秘密のメモリ領域におけるエントリだけが検査され、このエントリに依存してスタンダードの場合とアプリケーションの場合との間で切り換えられる。つまり、検査メカニズムが活性化されるか乃至は不活性化される。秘密のメモリ領域にエントリが存在しない場合、スタンダードの場合から出発して、検査メカニズムが活性化される。従って、公知の制御機器では相応のエントリによる秘密のメモリ領域の書き込みによってスタンダードの場合からアプリケーションの場合に切り換えられる。

【０００９】しかし、秘密のメモリ領域の書き込みによるスタンダードの場合からアプリケーションの場合への切り換え過程は公知の制御機器では比較的問題ないと言える。この場合、特に興味深いのはアプリケーション機器の秘密のメモリ領域に格納されているエントリであ

る。マイクロコンピュータシステムのメモリ装置に格納されたデータの活性化又は不活性化のための従来技術から公知の方法では、エントリがアプリケーション機器から読み出され、更に別の制御機器を不活性化された検査メカニズムを有するアプリケーションの場合に切り換えるために利用されてしまうかもしれない。これらの不正操作されたアプリケーション機器において、不正操作されたデータが格納され、次いでこれらの不正操作されたデータが実行乃至は利用されてしまうかもしれない。これらの不正操作されたデータが確実に利用されないようにすることはできない。

【0010】

【発明が解決しようとする課題】それゆえ、本発明の課題は、資格のない第三者によるメモリ装置に格納されたデータの不正操作のために、これらの不正操作されたデータの利用を確実にかつ効果的に阻止することである。

【0011】

【課題を解決するための手段】上記課題は、冒頭に記載されたタイプの方法において、以下の方法ステップ、すなわちマイクロコンピュータ固有の識別子は暗号化されるか又はマイクロコンピュータ固有の識別子の署名がメモリ装置の予め設定可能なメモリ領域に格納される方法ステップ、マイクロコンピュータシステムの起動の際に識別子の署名が検査され乃至は識別子が復号化される方法ステップ、署名の検査の結果に依存して乃至は復号化された識別子に依存してデータの少なくとも一部分が活性化又は不活性化される方法ステップによって解決される。

【0012】さらに、上記課題は、冒頭に記載されたタイプのマイクロコンピュータシステムにおいて、メモリ装置の予め設定可能なメモリ領域に署名されて又は暗号化されて格納されたマイクロコンピュータ固有の識別子を有し、マイクロコンピュータシステムの起動時に識別子の署名の検査のための乃至は識別子の復号化のための手段を有し、マイクロコンピュータシステムのメモリ装置に格納されたデータの少なくとも一部分を署名の検査の結果乃至は復号化された識別子に依存して活性化又は不活性化するための手段を有することによって解決される。

【0013】

【発明の実施の形態】本発明によれば、メモリ装置のメモリ領域へのエントリが署名乃至は暗号化されている。このエントリはメモリ装置の任意のメモリ領域に格納される。暗号化されたエントリの格納は再プログラミング又は変更プログラミングに引き続いて行われるか又は相応の方法をきっかけとして行われる。本発明の方法の安全性はとりわけ秘密鍵によるエントリの署名又は暗号化によって与えられ、メモリ領域のアドレスの秘密保持によっては与えられない。このメモリ領域はメモリ装置の再プログラミングの際にクリアされるが、新しいデータによって書き込まれてはならない。マイクロコンピュータシステムは例えば自動車機能の開ループ制御及び/又は閉ループ制御のための制御機器として構成されている。

【0014】マイクロコンピュータシステムの起動の際にエントリの署名が検査されるか乃至はエントリが復号化される。メモリ領域にエントリが存在しないか又はそこに格納されたエントリの署名の検査又はエントリの復号化が失敗した場合には、スタンダードの場合から出発して、検査メカニズムが活性化される。これに対して、メモリ領域に格納されたエントリの署名の検査又はエントリの復号化が成功した場合には、アプリケーションの場合から出発して、検査メカニズムが不活性化される。すなわち、本発明ではメモリ装置の予め設定可能なメモリ領域における相応の暗号化されたエントリの格納によってスタンダードの場合からアプリケーションの場合に切り換えられる。

【0015】本発明の方法によって制御機器はスタンダードの場合とアプリケーションの場合との間で切り換えられるだけではない。メモリ領域における暗号化されたエントリを介してデータの任意の部分すなわちプログラムの任意の機能を活性化乃至は不活性化することも考えられる。これによって例えば自動車製造者は自動車制御機器の制御プログラムへの所期の介入によって様々な自動車機能、例えば内燃機関の様々な性能を実現することができる。従って、本発明によって、プログラムの任意の機能が、資格のある人物のみによって操作されるソフトウェアスイッチを介して活性化乃至は不活性化される。

【0016】本発明の有利な実施形態によれば、データの異なる部分の活性化又は不活性化のために様々な識別子がメモリ装置のメモリ領域に格納されることが提案される。よって、プログラムの様々な機能はメモリ領域の内容を介して活性化乃至は不活性化される。

【0017】本発明の他の有利な実施形態によれば、データの異なる部分の活性化又は不活性化のために識別子がメモリ装置の様々なメモリ領域に格納されることが提案される。よって、プログラムの様々な機能は識別子が格納されているメモリ領域を介して活性化乃至は不活性化される。様々な識別子を様々なメモリ領域に格納することも考えられ、この結果、こうしてできるだけ少ないメモリ占有面積によってできるだけ多くのプログラム機能を活性化乃至は不活性化することができる。

【0018】本発明の有利な実施形態によれば、限定されたユーザグループだけがアクセス可能なプライベート鍵に基づいてマイクロコンピュータ固有の識別子が署名又は暗号化され、自由にアクセス可能な公開鍵に基づいて識別子の署名が検査されるか乃至は識別子が復号化されることが提案される。この実施形態によれば識別子は非対称鍵暗号化方法に従って署名乃至は暗号化される。

非対称鍵暗号化方法は公開鍵暗号化方法とも呼ばれる。非対称鍵暗号化方法は例えばRSA（この方法の開発者Ronald Rivest, Adi Shamir及びLeonard Adlemanによって名付けられた；モジュロの累乗c＝m^e mod nによる暗号化）、LUC（RSAに似ている；ルーカス数列の形成による暗号化）又はMNLN（Mueller, Noebauer, Lidl,Noebauer；RSAに似ているが、多項式x^eがディクソン多項式によって置き換えられる）（http://www.unlmalnz.de/ipommeren/DSVorlesung/KryptoBasis/asymmetrisch.html を参照）である。

【0019】非対称鍵暗号化方法では、例えば自動車の制御機器のための制御プログラムの署名のために、署名すべき制御プログラム及び/又は署名すべきデータからハッシュ関数によってハッシュ値が形成される。ハッシュ値は、使用されるハッシュ関数に依存する特別な特性を有するある種のチェックサムである。ハッシュ値は自由にアクセスできないプライベート鍵によって暗号化される。暗号化されたハッシュ値は署名と呼ばれる。署名は署名すべきプログラム及び/又は署名すべきデータに付加され、これと一緒に自動車制御機器に伝送され、そこでメモリ装置に格納される。

【0020】制御機器では署名が自由にアクセスできる公開鍵によって復号化される。これによって復号化されたハッシュ値が得られる。さらに暗号化の枠内でハッシュ値をもとめるために使用された同じハッシュ関数によって受信された制御プログラム及び/又は受信されたデータから更なるハッシュ値がもとめられる。次いで、復号化されたハッシュ値がこの更なるハッシュ値と等しいかどうかが検査される。等しい場合には、伝送された制御プログラムの実行乃至は伝送されたデータの利用が開始される。さもなければ、制御プログラムの実行乃至はデータの利用が阻止される。

【0021】有利には、データの利用中に変更されないメモリ装置のメモリ領域に識別子が格納される。よって、このメモリ領域にはプログラムの実行中に読み出しアクセスも書き込みアクセスも行われない。

【0022】有利には、メモリ装置の再プログラミングの枠内でクリアされるメモリ領域に識別子が格納される。よって、メモリ装置の再プログラミングに続いて、マイクロコンピュータ固有の識別子がメモリ装置の予め設定可能なメモリ領域に署名又は暗号化されて格納されなければならない。このために一方でマイクロコンピュータシステムの固有の識別子及び他方で正しい暗号化アルゴリズム及び正しい鍵が既知でなければならない。よって、再プログラミングされたデータの実行又は利用は、正しい識別子が正しい鍵及びアルゴリズムによって署名又は暗号化されてメモリ装置のメモリ領域に格納された場合にのみ阻止されない。

【0023】本発明の有利な実施形態によればマイクロコンピュータシステムの起動毎に識別子の署名が検査されるか乃至は識別子が復号化されることが提案される。

【0024】有利には、マイクロコンピュータシステムに割り当てられたシリアルナンバー、とりわけマイクロコンピュータシステムの計算機器に割り当てられたシリアルナンバーがメモリ装置の予め設定可能なメモリ領域に署名又は暗号化されて格納される。

【0025】本発明の有利な実施形態によれば、メモリ装置のメモリ領域に識別子が格納されていない場合又はそこに格納された識別子の署名の検査又はそこに格納された識別子の復号化がマイクロコンピュータシステムの起動時に失敗した場合に、マイクロコンピュータシステムにおいてメモリ装置に格納されたデータの不正操作を検査するためのメカニズムが活性化されることが提案される。よって、これらの場合には自動車制御機器として形成されたマイクロコンピュータシステムはスタンダードの場合に切り換えられる。設けられた検査メカニズムがデータの不正操作を識別する場合、再プログラミングされたデータの実行又は利用が阻止される。

【0026】本発明の有利な実施形態によれば、メモリ装置のメモリ領域に格納された識別子の署名の検査又はそこに格納された識別子の復号化がマイクロコンピュータシステムの起動時に成功した場合には、マイクロコンピュータシステムにおいてメモリ装置に格納されたデータの不正操作を検査するためのメカニズムが不活性化されることが提案される。よって、この場合には、自動車制御機器として構成されたマイクロコンピュータシステムがアプリケーションの場合に切り換えられる。

【0027】本発明の有利な実施形態によれば、マイクロコンピュータシステムは自動車機能の開ループ制御及び/又は閉ループ制御のための自動車の制御機器として構成されるように提案される。

【0028】本発明の有利な実施形態によれば、マイクロコンピュータシステムは本発明の方法を実施するための手段を有するように提案される。

【0029】有利には、計算機器で実行可能であり、本発明の方法を実施するのに適したコンピュータプログラムがメモリ装置に格納されている。

【0030】有利には、メモリ装置は計算機器と同一の半導体構成素子に形成されている。このようないわゆるワンチップメモリにおいてはプログラムメモリ乃至はこのメモリに格納されたデータは外部から不正操作され得ない。これによってマイクロコンピュータシステムはさらにメモリ装置に格納されたデータの不正操作から保護される。

【0031】

【実施例】図面に基づいて以下において本発明の実施例を説明する。

【0032】本発明の対象はマイクロコンピュータシステムのメモリ装置に格納されているデータの少なくとも一部分を活性化又は不活性化するための方法である。マ

イクロコンピュータシステムは例えば所定の自動車機能を開ループ制御及び/又は閉ループ制御するための自動車の制御機器として構成されている。データは例えば制御プログラムとして、限界値として、パラメータ値として構成される。

【００３３】制御プログラムの部分の活性化乃至は不活性化によって制御機器の様々な機能がスイッチオン乃至はオフされる。とりわけ制御プログラムの部分の活性化乃至は不活性化によって制御機器がスタンダードの場合からアプリケーションの場合に切り換えることが顧慮される。スタンダード機器の場合、制御機器のメモリ装置に格納されたデータの不正操作の検査のためのメカニズムが活性化されている。不正操作されたデータはこれらのメカニズムによって識別され、これらのデータは阻止される。これらのメカニズムは全く異なるように構成することができる。従来技術からは多数の異なる検査メカニズムが公知である。様々なデータが迅速にかつ簡単にメモリ装置に格納されるように、所定の状況において、とりわけ制御機器の開発及びテストフェーズの間には検査メカニズムを不活性化することが必要である。不活性化された検査メカニズムを有する制御機器はアプリケーション機器と呼ばれる。

【００３４】図１に図示された本発明の方法は機能ブロック１から始まる。機能ブロック２においてマイクロコンピュータ固有の識別子が非対称鍵暗号化方法によるプライベート鍵によって署名又は暗号化される。署名又は暗号化された識別子は証明書（certificate）と呼ばれる。識別子は例えば制御機器又は計算機器、とりわけ制御機器のマイクロプロセッサのシリアルナンバーである。識別子の暗号化は図２に基づいて詳しく記述する。機能ブロック３では制御機器の起動時に公開鍵によって識別子の署名が検査されるか乃至は識別子が復号化される。問い合わせブロック４では識別子の署名が適切であるかどうか又は復号化された識別子がマイクロコンピュータシステムの実際の識別子と一致しているかどうかが検査される。イエスの場合には、この制御機器はアプリケーション機器であり、機能ブロック５において全検査メカニズムが不活性化される。しかし、メモリ領域に識別子が存在しない場合、署名が間違っているか又は復号化された識別子が実際の識別子と一致していない場合には、この制御機器はスタンダード機器であり、機能ブロック６において検査メカニズムが活性化される。メモリ装置に格納されたデータの将来の実行又は利用の際にこれらのデータは不正操作されていないかどうか検査される。通常は不正操作されたデータが識別され阻止され、この結果、実行又は利用はもはや不可能である。よって、機能ブロック３～６において、識別子に依存して制御プログラムの部分が活性化乃至は不活性化される。機能ブロック７で本発明の方法は終了する。

【００３５】図２には図１の方法の更に別のフローチャートが図示されており、とりわけデータの署名乃至は暗号化及び署名の検査乃至はデータの復号化が詳しく示されている。制御機器のマイクロプロセッサのシリアルナンバー１０から機能ブロック１１においてハッシュ関数によっていわゆるハッシュ値１２が形成される。ハッシュ値１２は機能ブロック１３においてプライベート鍵１４によって暗号化される。暗号化されたハッシュ値は署名１５と呼ばれる。署名１５はシリアルナンバー１０に付加され、これら両方が適当なデータインターフェースを介して自動車の制御機器に伝送され、そこでメモリ装置の予め設定されたメモリ領域に格納される。

【００３６】制御機器ではシリアルナンバー１０が署名１５から分離される。署名１５は機能ブロック１６において公開鍵１７によって復号化される。復号化されたハッシュ値は参照符号１８で示されている。機能ブロック１９においてシリアルナンバー１０から機能ブロック１１で使用されたのと同一のハッシュ関数に基づいて更に別のハッシュ値２０がもとめられる。問い合わせブロック２１において、復号化されたハッシュ値１８がもとめられたハッシュ値２０に等しいかどうか、すなわち復号化されたシリアルナンバーが制御機器のマイクロプロセッサの実際のシリアルナンバー１０に等しいかどうかが検査される。イエスの場合にはこの制御機器はアプリケーションの場合に切り換えられる。このためにメモリ装置に格納されたデータを不正操作に関して検査するための検査メカニズム３５、３６は問い合わせブロック２１によって制御されるスイッチング素子２２によって不活性化される。さもなければ、検査メカニズム３５、３６がスイッチング素子２２によって活性化されることによって、この制御機器はスタンダードの場合に切り換えられる。

【００３７】プライベート鍵１４は限定されたユーザーグループだけが自由に使用できる。安全性を高めるために、プライベート鍵１４をトラストセンタ（Trust-Centre）で管理し、シリアルナンバー１０をこのトラストセンタの署名サーバによって署名することが考えられる。相応の方法は出願日２００１年５月１２日の同一の出願人の別個の特許出願ＤＥ１０１２３１６９にも記述されている。この出願の内容に明らかに関係する。

【００３８】代替的に、識別子１０をプライベート鍵１４によって直接暗号化してもよい。暗号化された識別子は制御機器に伝送され、そこで公開鍵１７によって直接復号化される。復号化された識別子１０に依存してこの制御機器においてスイッチング素子２２を介してメモリ装置に格納されたデータの少なくとも一部分が活性化又は不活性化される。

【００３９】図３には本発明のマイクロコンピュータシステムの全体が参照符号３０で示されている。マイクロコンピュータシステム３０は自動車機能の開ループ制御及び/又は閉ループ制御のための自動車の制御機器とし

て構成されている。この制御機器３０はとりわけマイクロプロセッサとして構成されている計算機器３１及びメモリ装置３２を有する。このメモリ装置３２には様々なデータ３３、とりわけ制御プログラム、限界値又はパラメータ値が格納されている。メモリ装置３２はマイクロプロセッサ３１と同じ半導体構成素子に形成される（ワンチップメモリ）。メモリ装置３２の予め設定可能なメモリ領域３４にはマイクロコンピュータ固有の識別子１０、とりわけマイクロプロセッサ３１のシリアルナンバー（ＣＰＵシリアルナンバー）が署名又は暗号化されて格納されている。メモリ領域３４はメモリ装置３２の再プログラミングの枠内で自動的にクリアされるが、新しいデータによって書き込まれない。データ３３の利用中に、すなわち制御プログラムの実行中に、メモリ領域３４の内容は変更されない。

【００４０】制御機器３０の起動の際に識別子１０の署名１５が検査されるか乃至は識別子１０が復号化される。このために制御機器３０にはこの制御機器３０の起動毎にメモリ領域３４の内容を検査する適当な手段が設けられている。メモリ領域３４の内容に依存して制御機器３０の相応の手段によって制御プログラム３３の所定の部分３５、３６が活性化乃至は不活性化される。これらの部分３５、３６は例えば検査メカニズムであり、これらの検査メカニズムによってメモリ装置３４に格納された他のデータ３３が不正操作されていないか検査される。

【００４１】メモリ領域３４に識別子１０、１５が格納されていない場合又は署名１５の検査又は識別子１０の復号化により識別子１０、１５が間違ったプライベート鍵１４によって署名されているか又は暗号化されていることが明らかになった場合、制御プログラム３３の部分３５、３６が活性化されることによって制御機器３０はスタンダードの場合に切り換えられる。さもなければ、制御プログラム３３の部分３５、３６が不活性化されることによって制御機器３０はアプリケーションの場合に切り換えられる。

【００４２】制御機器３０を市場に供給する際には、メモリ装置３２のメモリ領域３４は空白である。従って、これは活性な検査メカニズムを有するスタンダード機器である。スタンダード機器が不活性な検査メカニズムを有するアプリケーション機器に切り換えられなければならない場合に、制御機器３０のマイクロプロセッサ３１のシリアルナンバーが署名又は暗号化されてメモリ領域３４に格納される。このために、限定されたユーザグループだけがアクセスできる正しいプライベート鍵１４が必要である。

【００４３】有利には、メモリ装置３２にはコンピュータプログラムが格納されており、このコンピュータプログラムは計算機器３１において実行可能であり、以下の方法ステップを実行するのに適している：署名された又は暗号化されたマイクロコンピュータ固有の識別子１０、１５をメモリ装置３２の予め設定可能なメモリ領域３４に格納する方法ステップ；マイクロコンピュータシステム３０の起動の際に識別子１０の署名１５の検査乃至は識別子１０の復号化を行う方法ステップ；メモリ領域３４の内容に依存してメモリ装置３２に格納されたデータの少なくとも一部分を活性化乃至は不活性化する方法ステップ。

【００４４】よって、メモリ装置３２に格納されたデータは署名１５の検査の結果に依存して乃至は復号化された識別子１０に依存して活性化乃至は不活性化される。

【図面の簡単な説明】

【図１】実施例による本発明の方法のフローチャートである。

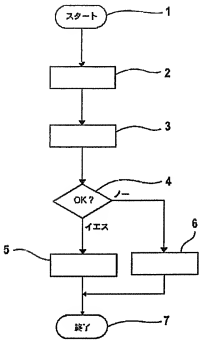
【図２】図１の方法の更に別のフローチャートである。

【図３】実施例による本発明のマイクロコンピュータシステムの概略図である。

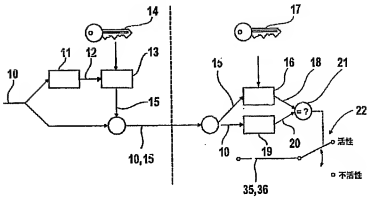
【符号の説明】

１０　識別子、シリアルナンバー
１２　ハッシュ値
１４　プライベート鍵
１５　署名
１７　公開鍵
１８　復号化されたハッシュ値
２０　更に別のハッシュ値
２２スイッチング素子
３０　マイクロコンピュータシステム
３１　計算機器、マイクロプロセッサ
３２　メモリ装置
３３　データ、制御プログラム
３４　メモリ領域
３５、３６　制御プログラムの部分

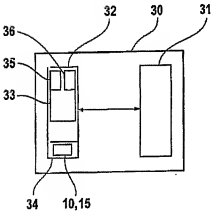
【図１】



【図２】



【図３】



フロントページの続き

(72)発明者　ラルフ　アングルバウアー
ドイツ連邦共和国　シュツツトガルト　アウシュトラーセ　113

(72)発明者　アレキサンダー　ハインドル
オーストリア国　ヴィーン　ヴィルヘルムーエクスナーガッセ　14／9

Fターム(参考)　5B017 AA07 BA08 CA04